

REMARKS

Claims 16-30 and 128-132 were previously pending in this application. Reconsideration of presently pending claims 16-30 and 128-132 is respectfully requested in light of the following comments.

Rejections under 35 U.S.C. §112

Claims 16-30, 128, 131, and 132 were rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. More specifically, the Office indicated that the omitted element is the key distribution center. (Office Action, pg. 2). Applicant respectfully disagrees. The Present Application specifies that “the central key distribution center 1024 of the communication network 1000 may be distributed among a plurality of functional elements, including the home agent 1010 and the home AAA server 1018.” (Present Application, pg. 31) (emphasis added). Therefore, the rejection of claims 16-30, 128, 131, and 132 under 35 U.S.C. §112, second paragraph, should be withdrawn.

Rejections under 35 U.S.C. §103

Claims 16-30 and 128-132 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Inoue et al. (U.S. Patent 6,167,513 hereinafter referred to as “Inoue”) in view of RFC 1827 IP Encapsulating Security Payload (ESP) (hereinafter referred to as “RFC 1827”) and in further view of Lewis (U.S. Patent 6,453,159 hereinafter referred to as “Lewis”). Applicant traverses these rejection on the grounds that these reference are defective in establishing a *prima facie* case of obviousness with respect to the claims.

In *KSR Int’l. Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1739 (2007), the Court stated that

a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. Although common sense

directs one to look with care at a patent application that claims as innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. This is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known. *Id.* at 1741 (emphasis added).

As the PTO recognizes in MPEP § 2142:

... The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness...

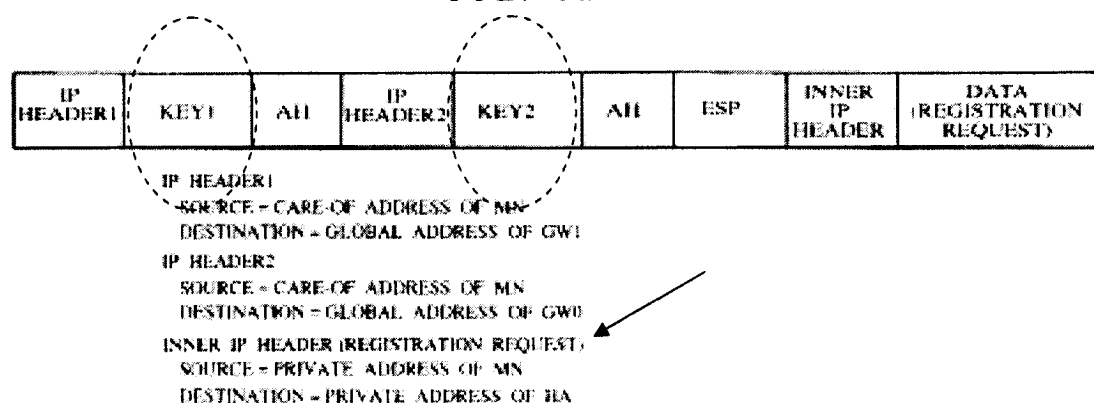
It is submitted that, in the present case, the Examiner has not factually supported a *prima facie* case of obviousness for the following reasons.

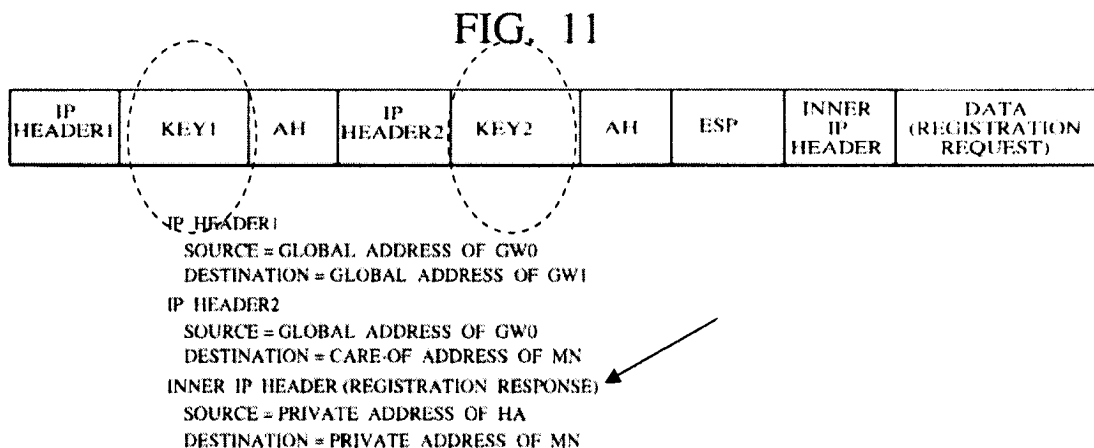
THE ELEMENTS BEING COMBINED ARE NOT PERFORMING THEIR KNOWN OR ESTABLISHED FUNCTION

KSR teaches that when combining elements from different references, it is important to determine whether the element is performing “the same function it had been known to perform.” *KSR* at 1740. It is clear that the encryption/authentication method of Inoue should not be combined with the encryption key request method of Lewis because the known functions of the encryption/end-to-end authentication format and encryption/link authentication format of Inoue are changed.

More particularly, Inoue discloses that a mobile computer transmits a registration request message (shown below in FIG. 10) in the encryption/end-to-end authentication format and encryption/link authentication format which includes encryption keys KEY1 and KEY2. Accordingly, Inoue discloses that the registration request message can be authenticated by the gateways (GW1 and GW0) of the foreign network and the home network so that the request can be passed to the home agent (HA) for registering the mobile terminal in the foreign network. The home agent (HA) is then able to send a registration response message (shown below in FIG. 11) which also includes the encryption keys KEY1 and KEY2 so that the response can be pass to the mobile terminal via gateways GW0 and GW1 in a similar manner. Thus, the encryption keys of Inoue are already provided prior to the mobile computer transmitting a registration request in order to have a secure communication pathway to and from the home agent.

FIG. 10





In contrast, Lewis discloses that a mobile terminal must register with a respective access point in order to carry out wireless communications with devices on a system backbone. Assuming *arguendo*, that the access point of Lewis can be seen as a home domain as is alleged by the Examiner. (Office Action, pgs. 7 and 12). As such, the mobile terminal sends a request to register with the access point. If the mobile terminal does not provide an ENCRYPT key in the request, the mobile terminal sends a “GET KEY” command to the access point requesting that the network encryption key, ENCRYPT key, be provided. (Lewis, Col. 18, lines 3-11). The access point then transmits a request for the ENCRYPT key to a key distribution server. (Lewis, Col. 18, lines 15-17). In response, the key distribution server transmits the ENCRYPT key to the requesting mobile terminal via the access point. (Lewis, Col. 18, lines 19-21).

As noted above, there would be no reason for the home agent of Inoue to request encryption keys from the key distribution server as is taught in Lewis since the encryption keys are already provided in the registration request message sent from the mobile computer to the home agent. Since this modification of the Inoue reference clearly destroys the purpose or function of the invention disclosed in the patent, one of ordinary skill in the art would not have found a reason to make the claimed modification.

Thus, for this reason alone, the Examiner's burden of factually supporting a *prima facie* case of obviousness has clearly not been met, and the rejection of claims 16-30 and 128-132 under 35 U.S.C. §103 should be withdrawn.

**THE EXAMINER HAS NOT SHOWN HOW THE ELEMENTS BEING COMBINED
PRODUCE A PREDICTABLE RESULT**

MPEP 2143.01 (III) states that the "mere fact that references can be combined does not render the resultant combination obvious unless the results would have been predictable to one of ordinary skill in the art." In the present case, the Examiner has not expressed any reason why combining the encryption/ authentication method of Inoue with the encryption key request method of Lewis in the way as claimed would produce a predictable result. The Office Action only indicated that "[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of [Inoue] and RFC-1827 a mobile communication scheme using encryption and authentication that utilizes RFC 1825-1829 schemes to include means for the home domain to request encryption keys." (Office Action, pg. 7). However, as discussed above, there would be no reason for the home agent of Inoue to request encryption keys (as alleged by the Examiner) since the encryption keys are already provided in the registration request message sent from the mobile computer to the home agent.

Thus, for this reason alone, the Examiner's burden of factually supporting a *prima facie* case of obviousness has clearly not been met, and the rejection of claims 16-30 and 128-132 under 35 U.S.C. §103 should be withdrawn.

**PRIOR ART THAT TEACHES AWAY FROM THE CLAIMED INVENTION CANNOT
BE USED TO ESTABLISH OBVIOUSNESS**

KSR maintained the long-standing principal that "when the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be non-obvious." *KSR Int'l. Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1740 (2007). In the present case the Inoue reference, by providing that encryption keys are included in a registration

request message (in the encryption/end-to-end authentication format and encryption/link authentication format) sent from a mobile computer in a foreign network to a home agent in a home network, clearly teaches away from using the encryption key request method of Lewis in order for the mobile terminal to access a network via an access point.

Thus, for this reason alone, the Examiner's burden of factually supporting a *prima facie* case of obviousness has clearly not been met, and the rejection of claims 16-30 and 128-132 under 35 U.S.C. §103 should be withdrawn.

ALL WORDS IN THE CLAIM MUST BE CONSIDERED

The cited references, alone or in combination, cannot be applied to reject claims 128-132 under 35 U.S.C. § 103(a) which provides that:

A patent may not be obtained ... if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains ... (Emphasis added)

MPEP §2143.03 states that “[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art.” (Quoting *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970)). Thus, when evaluating a claim for determining obviousness, all limitations of the claim must be considered. However, Applicant respectfully submits that the cited references, alone or in combination, do not teach a method of providing secure communication between a mobile node and home domain using a foreign domain that includes the feature of “requesting and receiving, by the home domain, a plurality of encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain,” as is recited in claims 128-132.

More specifically, the Office admits that the Inoue and RFC 1827 references do not

disclose “requesting and receiving, by the home domain, a plurality of encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain.” (Office Action, pg. 12). To cure the deficiencies of Inoue and RFC 1827, the Office points to Lewis in Col. 18, line 11 through Col. 19, line 35 as allegedly disclosing such a feature. Applicant respectfully disagrees. The Office indicated Lewis “teaches that an access point (i.e. home domain) requests an encryption key from a distribution key server when a mobile roams (i.e. foreign network).” (Office Action, pg. 12) (emphasis added).

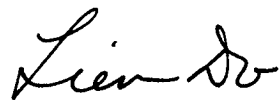
However, claims 128-132 recite that “a plurality of encryption keys” are requested and the encryption keys are “for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain.” In contrast, Lewis discloses when the mobile terminal does not have the network encryption key, one ENCRYPT key, the mobile sends a “GET KEY” command to the access point. (Lewis, Col. 18, lines 3-11). The access point then “transmits a request for the ENCRYPT key to the key distribution server in association with the mobile terminal requesting association.” (Lewis, Col. 18, lines 15-17). After the mobile terminal receives the ENCRYPT key, the mobile may use this key to complete association with the access point in order to access and communicate with devices on a system backbone. (Lewis, Col. 18, lines 28-31). Accordingly, the Lewis reference does not teach the feature of “requesting and receiving, by the home domain, a plurality of encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain.”

Thus, for this reason alone, the Examiner’s burden of factually supporting a *prima facie* case of obviousness has clearly not been met, and the rejection of claims 28-132 under 35 U.S.C. §103 should be withdrawn.

Conclusion

It is clear from all of the foregoing that claims 16-30 and 128-132 are in condition for allowance. Favorable consideration and an early indication of allowability are respectfully requested. The Examiner is invited to call the undersigned at the below-listed number if a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,



Liem T. Do
Registration No. 59,804

Dated: 2/5/09

HAYNES AND BOONE, LLP
Telephone: 972/739-8643
Facsimile: 214/200-0853
Customer No.: 27683
Client Matter No.: 22171.321/11349RR
R-220829

I hereby certify that this correspondence is being electronically filed with the U.S. Patent and Trademark Office via EFT-Web System on the date indicated below.

on: Feb. 5, 2009
Bonnie Boyle
Bonnie Boyle